IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY
TRENTON DIVISION

ALICIA COOPER, on behalf of herself and all others similarly situated,	:	Civil Action No. _____
Plaintiff,	:	
vs.	:	CLASS ACTION
HEARTLAND PAYMENT SYSTEMS, INC.,	:	
Defendant.	:	JURY TRIAL DEMANDED

COMPLAINT

Plaintiff Alicia Cooper ("Plaintiff"), on behalf of herself and all others similarly situated, by and through her attorneys, allege as follows:

INTRODUCTION

1. This is a class action lawsuit brought on behalf of Plaintiff, individually, and on behalf of similarly situated consumers or entities whose credit and/or debit card number(s), expiration date(s), internal bank codes, personal identifying information and/or other confidential financial information (the "Sensitive Financial Information") was stolen, accessed and/or compromised by third parties while entrusted to Defendant Heartland Payment Systems, Inc. ("Heartland" or "Defendant"). Defendant Heartland processes credit card transactions and provides other services for over 250,000 businesses across the

United States, including restaurants and retail stores. Heartland handles approximately 100 million credit card transactions per month. In connection with its operations, Heartland comes into the possession of – and is entrusted with – the Sensitive Financial Information of millions of consumers from across the country.

2. Sometime in 2008, unknown and unauthorized third persons hacked into Heartland's computer network and gained access to the Sensitive Financial Information of an undetermined number of consumers.

3. Heartland only became aware of the data breach after it was notified of patterns of fraudulent credit card activity by Visa and MasterCard. Analysts have stated that the fact that Heartland did not detect the breach on its own suggests that it had not implemented (or was not using) all of the security controls called for by the Payment Card Industry Data Security Standard ("PCI"), a set of security controls mandated by the major credit card companies.

4. Heartland apparently learned that its computer systems might have been hacked in late October of 2008, and only determined that its systems had indeed been breached in mid January 2009. On January 20, 2009 – the date of the Presidential Inauguration – Heartland silently issued a press release that publicly revealed for the first time that a data breach had occurred. In addition to the questionable timing of this disclosure, there are materially misleading statements and omissions contained in Heartland's public description of the breach and its consequences.

5. While it has belatedly disclosed the data breach, Heartland has refused to identify which of its merchants are affected by the breach. Upon information and belief, Heartland has also failed to personally notify the consumers whose Sensitive Financial Information in a sufficiently timely manner, as required under various state statutes that require notice of a data breach without unreasonable delay.

6. The Sensitive Financial Information that was compromised in the Heartland data breach – which reportedly includes names and all of the information contained on a credit card's magnetic strip – can be used to make fake credit cards.

7. While Heartland has advised cardholders to carefully monitor their credit card statements and has set up a website with information regarding the data breach, it has not offered affected consumers *anything* that may protect or compensate them for their injuries suffered as a result of the breach, such as free credit monitoring, identity theft insurance, or payments for freezing/unfreezing one's credit.

8. Heartland has not revealed the number of consumers whose Sensitive Financial Information has been compromised. However, analysts have stated that the data breach at Heartland may rank among the biggest ever reported.

9. Upon information and belief, Heartland failed to take appropriate measures to adequately protect this Sensitive Financial Information. Indeed, shortly after the breach Heartland publicly disclosed that it would be taking numerous new measures to improve the security of its processing systems.

10. Plaintiffs bring this lawsuit for the purpose of securing full, appropriate, and meaningful relief based on Defendant's negligent, reckless, wrongful, and unlawful conduct, to wit:

a. *First*, Plaintiff seeks relief based on the injuries suffered by her and members of the Class as a result of Defendant failing to provide adequate safeguards to protect its customers' data, which would have prevented such a widespread security breach from occurring in the first place. Plaintiff also seeks prospective equitable relief to ensure that Heartland takes necessary measures to make certain that such massive data breaches do not reoccur in the future.

b. *Second*, Plaintiff seeks appropriate relief for Heartland's inexplicable delay, questionable timing, and inaccuracies concerning the disclosures about the security breach that reportedly occurred as early as the Fall of 2008. Plaintiff likewise seeks relief for damages caused by Heartland's negligence in taking months to determine the existence and scope of the data breach. These unreasonable delays prevented and/or hindered Plaintiff and members of the Class from taking immediate steps to monitor and attempt to safeguard their financial information.

c. *Third*, Plaintiff seeks meaningful and appropriate relief on behalf of herself and the Class. Heartland is offering Plaintiff and

putative class members *nothing*. Plaintiff further seeks to ensure that all of the affected consumers receive prompt, complete, and accurate disclosures regarding the loss of their Sensitive Financial Information that includes, without limitation, details of exactly what information was compromised, an explanation of how the breach occurred, and an assurance that it has been completely contained.

11. As a result of Defendant's wrongful conduct, possibly millions of consumers across the United States have had their Sensitive Financial Information compromised, have had their privacy rights violated, have experienced unauthorized credit card charges, have been exposed to the risk of fraud and identity theft, and have otherwise suffered damages. These damages include, without limitation, the cost of obtaining identity theft insurance, the cost of obtaining credit reports to monitor for unauthorized transactions (to the extent that they are not free[1]), costs associated with canceling and obtaining new credit and debit cards, the loss of Class members' control of the Sensitive Financial Information, costs associated with "freezing" and "unfreezing" a consumers' credit accounts more than once, the cost of placing an additional freeze after a certain period of times, fear and apprehension of fraud, loss of money and identity theft, the burden of closely scrutinizing account statements and credit reports for unauthorized activity, and other economic and non-economic damages.

[1] Consumers are entitled to a single free credit report once every 12 months.

12. Defendant Heartland's actions constitute violations of the consumer protection statute of New Jersey, and amount to a breach of implied contract, breach of fiduciary duty, negligence *per se*, and negligence.

PARTIES

13. Plaintiff Alicia Cooper is a resident of Woodbury, Minnesota. In or around January 23, 2009, Cooper was notified by her credit union that a card associated with her account was included in the Heartland data breach. A true and correct copy of the notification received by Cooper is attached hereto as Exhibit 1. As a proximate result of Defendants' conduct alleged herein, Cooper has suffered injuries. Specifically, Cooper's private, nonpublic financial information has been improperly and illegally compromised and/or disseminated to third parties as a result of Defendants' actions; Heartland has wrongfully prevented Cooper from taking prompt measures to protect herself through Heartland's unreasonable delay in identifying the breach and in notifying Cooper; and Heartland's failure to provide any remedies or protection is wholly insufficient to make Cooper whole or otherwise adequately protect her from identity theft, all of which has caused her to suffer from distress and disturbance to her peace of mind.

14. Defendant Heartland is a Delaware corporation with a principal place of business located at 90 Nassau Street, Princeton, New Jersey 08542.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this class action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005,

because the matter in controversy exceeds $5 million, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of states different than the Defendant. *See* 28 U.S.C. § 1332(d)(2)(A).

16. This Court has personal jurisdiction over Defendant Heartland because it owns and operates a business that is located within this state, and conducts substantial business throughout the United States.

17. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(a)(2) because a substantial part of the acts giving rise to Plaintiff's claims occurred in this district, and because Defendant is headquartered and conducts substantial business in this judicial district.

FACTUAL BACKGROUND

A. Hartland's Payment Systems and Other Services.

18. Heartland describes itself as "one of the nation's largest payment processors delivering credit/debit/prepaid card processing, payroll, check management and payments solutions." Since its founding in 1997, Heartland has grown to service 250,000 business locations nationwide with net sales of $1.3 billion in 2007. Securities of Heartland are publicly traded on the New York Stock Exchange under the ticker "HPY."

19. Heartland provides payment processing services related to bank card transactions for merchants throughout the United States and some parts of Canada. In addition, Heartland provides certain other merchant services, including check processing, the sale and rental of terminal equipment, and the sale of

terminal supplies. Heartland and its affiliates and subsidiaries also provide payroll and related tax filing services, prepaid card and "stored-value card solutions," and campus payment solutions throughout the United States. According to the company's most recent Form 10-K filed with the Securities and Exchange Commission, substantially all of the Heartland's revenue is derived from processing and settling Visa and MasterCard bank card transactions for its merchant customers.

20. On the website that it created in connection with its disclosure of the data breach,[2] Heartland claims to have a "proven track record of providing superior solutions to demanding markets such as pay-at-the-pump gas stations, parking lots, retail, restaurants, school campuses, hospitality businesses, and community banks. The company has also been effective in servicing auto repair facilities, convenience and liquor stores, and professional service providers."

21. In connection with the functions that it performs on behalf of its merchant clients, Defendant Heartland is provided and entrusted with the confidential Sensitive Financial Information of hundreds of millions of people. Many of Heartland's clients, such as retail stores, restaurants, and other merchants, contract with Heartland to administer services concerning their consumer customers.

22. Upon information and belief, Defendant has expressly or impliedly represented that it would take appropriate measures to safeguard the Sensitive Financial Information of Plaintiffs and Class members. For example, Heartland's

[2] www.2008breach.com.

website related to the data breach claims that "Heartland is deeply committed to maintaining the security of cardholder data, and we will continue doing everything reasonably possible to achieve this objective." Similarly, listed below Heartland's corporate logo are the phrases "The Highest Standards" and "The Most Trusted Transactions."

23. Plaintiffs and Class members are required to provide Heartland with their Financial Sensitive Information in order to get the benefit of Heartland's services. For example, customers of Heartland's merchant-clients who make a transaction with a debit or credit card provide this information to Heartland (via its customers) in order to process the payment.

B. The 2008 Data Breach.

24. Beginning at some point (or points) at least as early as 2008, Heartland's processing system was breached by a hacker. It has been reported that Heartland first learned that it "might have been hacked" in or around late October of 2008. According to its website, Heartland learned about the breach "[a]fter being alerted by Visa® and MasterCard® of suspicious activity surrounding processed card transactions…"

25. Upon information and belief, it took Heartland several months to confirm that its processing systems had indeed been breached after learning of this "suspicious activity." In early January 2009, after Heartland enlisted the help of "several forensic auditors to conduct a thorough investigation into the matter," it was discovered that "malicious software that compromised [the] data… [had]

crossed Heartland's network." This malicious software, which has the ability to record payment card transaction data, was reportedly intercepting transaction data as it was being sent to Heartland's in-house system for processing. A Heartland spokesperson has described the "malware" planted by the hackers as containing "extremely sophisticated code."

26. Heartland first publicly disclosed the breach on January 20, 2009 – amidst the flurry of media attention covering the Presidential Inauguration. Robert H.B. Baldwin, Jr., Heartland's president and chief financial officer, stated in a press release that was issued on that day: "[w]e understand that this incident may be the result of a widespread global cyber fraud operation, and we are cooperating closely with the United States Secret Service and Department of Justice."

27. Heartland has not been able to confirm that the breach has even been resolved; its website states "[w]e *believe* the intrusion is contained." (emphasis supplied).

C. Events Leading up to The Disclosure of The Breach.

28. It is clear that there are several steps that Heartland should and could have taken that might have prevented this breach from occurring. On its website related to the breaches, Heartland states – now that its processing systems have already been breached – that it is taking numerous measures to protect it going forward:

> **What are we doing to further secure our systems?**
> Heartland immediately took a number of steps to further secure its systems. In addition, Heartland will implement a next-generation program designed to flag network anomalies in real-

> time and enable law enforcement to expeditiously apprehend cyber criminals. Heartland is deeply committed to maintaining the security of cardholder data, and we will continue doing everything reasonably possible to achieve this objective.

29. Upon information and belief, beginning months ago Heartland sent letters to different credit card companies informing them of a data breach, and telling them to cancel certain credit card accounts. Upon information and belief, these credit card company customers then received letters informing them that their cards had been canceled.

D. Heartland's Failure to Provide Any Meaningful Relief to Class Members.

30. The measures taken by Heartland subsequent to the data breach fare no better than its conduct beforehand. Heartland has not offered any kind of relief such as free credit monitoring or other services that might prevent affected consumers from experiencing fraud or identity theft.

31. For what has been described as potentially the "largest data breach ever" – and which undisputedly includes very sensitive financial and banking information – Heartland has taken a caviler approach to the seriousness of this breach. Indeed, Baldwin recently described the breach as follows in an article:

> "The nature of the [breach] is such that card-not-present transactions are actually quite difficult for the bad guys to do because one piece of information we know they did not get was an address," Baldwin said. As a result, he said, the prospect of thieves using the stolen data to rack up massive amounts of fraud at online merchants "is not impossible, but much less likely."

32. It has been reported, however, that the information that was compromised in the Heartland data breach includes the digital information encoded

into the magnetic stripe built into the backs of credit and debit cards. This information is extremely lucrative to identity thieves, who can use it to create counterfeit credit cards by imprinting this information onto fabricated cards. Magnetic strips on the back of a credit or debit card often contain data like the primary account number, the user's name, a country code, an expiration date for the card and several characters of additional, discretionary data.

33. Heartland has also failed to reveal the names of the merchants whose customers are affected by the breach. Baldwin offered the following explanation for failing to reveal this information in an article that was posted on the *Washington Post*'s website:

> "No merchant of ours represents even [one-tenth of one percent] of our volume, and to put out any name associated with what is obviously an unfortunate incident is not fair. Their customers might end up having their cards used fraudulently, but that fraud might turn out to have come from their store, or it might be from another Heartland store and no one will ever really know."

34. Not only has Heartland kept its merchants (and their customers) in the dark publicly, but it also has not informed many of them in private. Indeed, many of Heartland's merchant/clients are anxiously seeking additional information about the breaches from Heartland. According to one article, Henry Helgeson, president and co-CEO of Merchant Warehouse Inc. (a Boston-based provider of payment card processing services and software) stated "[w]e're dying for information on this one. Everybody who processes card information is dying to know how exactly this happened."

35. Certain credit card companies and banks have stated that they do not have plans to re-issue new cards that may be affected by the breach. TD Banknorth, for example, has posted a security warning on its website that says "…at this time we do not have plans to re-issue cards which may be affected by this breach."

36. Many states require entities like Heartland that are subject to a data breach of this type to notify affected consumers that their Sensitive Financial Information has been compromised. Upon information and belief, Heartland has not provided *any* notice (other than its press release and website) to *any* consumers who were affected by the breach.

37. The very limited information that has been available about the data breach by Heartland is less than complete and fully accurate. For example, the list of "Frequently Asked Questions" on Heartland's website states what information was *not* impacted by the data breach, but does not list all of the information that was compromised.[3] Heartland describes itself as a "victim of a data breach" when, in light of its failure to adequately secure its processing systems, is also culpable. Heartland also makes the bold (and less than accurate) statement that "Cardholders are not responsible for unauthorized fraudulent charges made by third parties." Under the circumstances, these affirmative statements and omissions are materially misleading.

[3] For example, the Q&A lists the following exchange:

> **"Were cardholder Social Security numbers impacted?**
> No cardholder Social Security numbers, unencrypted personal identification numbers (PIN), addresses or telephone numbers were involved in the breach."

38. As a final insult to consumers whose information was compromised in the data breach, Heartland offers them an impersonalized apology for "any inconvenience this situation has caused," and "advises cardholders to examine their monthly statements closely and report any suspicious activity to their card issuers."

39. In the *Washington Post* Article, Heartland's Baldwin offered the following explanation why it was not appropriate for the company to offer consumers with any identity theft protection services:

> "Identity theft protection is appropriate when there is enough personal information lost that identity theft is possible," he said. "In this case, the amount of information we know they did not get is long enough that except in very circumscribed cases identity theft is just not possible. At the same time, we recognize and feel badly about the inconvenience this is going to cause consumers."

40. As a direct and proximate cause of Heartland's misconduct as described herein, Plaintiffs and Class members are at a substantially increased risk of fraud and identity theft. Indeed, Heartland itself has acknowledged that "suspicious activity surrounding processed card transactions" has already occurred.

CLASS ACTION ALLEGATIONS

41. This action is brought on behalf of Plaintiffs, individually and as a class action, pursuant to FED. R. CIV. P. 23(a), (b)(2) and (b)(3) on behalf of all consumers whose Sensitive Financial Information was provided to Heartland, and which was accessed and/or compromised. The Class does not include Defendant, or it officers, directors, agents, or employees.

42. Specifically, Plaintiffs seek to represent the following Classes:

> **Nationwide Class:** All persons in the United States whose Sensitive Financial Information was provided to Heartland, and which was accessed and/or compromised from either or both security breaches.

43. In the alternative, and pursuant to Fed. R. Civ. P. 23(c)(5), Plaintiffs seek to represent the following Sub-Classes:

> **New Jersey Sub-Class:** All persons residing in New Jersey whose Sensitive Financial Information was provided to Heartland, and which was accessed and/or compromised the data breaches.
>
> **Minnesota Sub-Class:** All persons residing in Minnesota whose Sensitive Financial Information was provided to Heartland, and which was accessed and/or compromised the data breaches.

44. The Nationwide Class is comprised of literally millions of consumers, the joinder of whom in one action is impracticable. Each of the Sub-Classes are likewise sufficiently large to make joinder impracticable. Disposition of the claims in a class action will provide substantial benefits to both the parties and the Court.

45. The rights of each member of the Class were violated in a similar fashion based upon Defendants' uniform actions.

46. Questions of law and fact common to the Class predominate over questions which may affect individual Class members, and include the following:

a. whether Defendant was negligent in collecting and storing the Sensitive Financial Information of Plaintiff and Class members;

b. whether Defendants owed a duty to Plaintiff and Class members to protect their Sensitive Financial Information;

c. whether Defendant breached this duty to exercise reasonable care in storing the Sensitive Financial Information of Plaintiff and Class members;

d. whether Defendant breached a duty by failing to keep Plaintiff and Class members' financial information secure;

e. whether Defendants' conduct violates the New Jersey Consumer Fraud Act;

f. whether Plaintiff and members of the Class are entitled to compensation, monetary damages, and/or any other services/corrective measure(s) from Heartland and, if so, the nature and amount of any such relief; and

g. whether statutory, punitive, and trebled damages are proper in this matter.

47. Plaintiff will fairly and adequately represent and protect the interests of the Class in that she has no interest that is antagonistic to or that irreconcilably conflicts with the interests of other members of any of the Classes.

48. Plaintiff has retained counsel competent and experienced in the prosecution of class action litigation.

49. Defendant has acted or refused to act on grounds generally applicable to Plaintiff and the Classes, thereby making appropriate equitable relief with respect to Plaintiff and the Classes as a whole.

50. A class action is superior to all other available methods for the fair and efficient adjudication of Plaintiff's and Class members' claims. Plaintiff and members of each class have suffered irreparable harm as a result of Defendant's deceptive, negligent, and unlawful conduct. The damages suffered by individual Class member may be relatively small, and thus few, if any individual class members can afford to seek legal redress on an individual basis for the wrong complained of herein. Absent a class action, Plaintiff and members of each of the Classes will continue to suffer losses as a result of Defendant's unlawful and negligent conduct, and will not be adequately protected and compensated therefore.

FIRST CAUSE OF ACTION
Violations Of New Jersey Consumer
Fraud Act ("NJCFA") (N.J.S.A. § 56:8-1 *et seq.*)
Asserted on Behalf of the Nationwide Class Against Heartland

51. Plaintiff repeats and realleges the allegations of the preceding paragraphs as if fully set forth herein.

52. Heartland, Plaintiff Cooper, and other members of the Class are "persons" within the meaning of the NJCFA.

53. Plaintiff Cooper and other members of the Class are "consumers" within the meaning of the NJCFA.

54. At all relevant times material hereto, Heartland conducted trade and commerce in New Jersey and elsewhere within the meaning of the NJCFA.

55. The NJCFA is, by its terms, a cumulative remedy, such that remedies under its provisions can be awarded in addition to those provided under separate statutory schemes.

56. Heartland has engaged in deceptive practices by *inter alia,* omitting, unreasonably delayed disclosing, and concealed material facts from its communications and disclosures to Plaintiff and all members of the Class regarding the nature and extent of the data breach.

57. The foregoing acts, misrepresentations, omissions and unconscionable commercial practices caused Plaintiff and other members of the Class to suffer an ascertainable loss and other damages.

SECOND CAUSE OF ACTION
NEGLIGENCE
Asserted on Behalf of the Nationwide Class Against Heartland

58. Plaintiff incorporates the allegations in the preceding paragraphs. This Count is brought on behalf of the **Nationwide Class.**

59. Defendant, upon coming into possession of Plaintiff and the Class' private, non-public, and financial information, had a duty to exercise reasonable care in safeguarding and protecting such information from being compromised and/or stolen. This duty arises from the common law, as well as from those duties expressly imposed upon Defendant from sources such as contracts between Plaintiff and Class members and third parties, agreements between Defendant and third parties, and industry standards (such as PCI).

60. Defendant also had a duty to timely and accurately disclose the fact that Plaintiff and the Class' private, non-public financial information within its possession had been, or was reasonably believed to have been, compromised.

61. Defendant also had a duty to have procedures in place to detect and prevent dissemination of Plaintiff's private information to third parties. This breach of security and unauthorized access was reasonably foreseeable to Heartland.

62. Defendant, through its acts and/or omissions, unlawfully breached their duty to Plaintiff and the Class by, *inter alia*, failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class' private, non-public Sensitive Financial Information within its possession.

63. Defendant, through its actions and/or omissions, breached their duty to Plaintiff and the Class by failing to have adequate procedures in place to detect and prevent dissemination of Plaintiff's private information to third parties.

64. Defendant, through its actions and/or omissions, breached their duty to timely disclose the fact that Plaintiff and the Class' private, non-public financial information within its possession had been, or was reasonably believed to have been, compromised.

65. But for Heartland's negligent and wrongful breach of its duties owed to Plaintiff and the Class, Plaintiffs' and the Class' private non-public financial information would not have been compromised. Further, but for Heartland's belated and incomplete revelations about the breaches, Plaintiff and Class members could have better protected themselves from the risk of identity theft and fraud.

66. Plaintiff and members of the Class' private, non-public, financial information was compromised, viewed, and/or stolen as the proximate result of Heartland failing to exercise reasonable care in safeguarding such information by

adopting, implementing, or maintaining appropriate security measures to protect and safeguard the private, non-public, and financial information within its possession.

67. Plaintiff and the Class have and/or can be expected to incur actual damages, including, but not limited to: expenses to prevent identity theft, expenses associated with freezing and unfreezing their credit reports, out-of-pocket expenses for identity theft coverage, credit monitoring, anxiety, emotional distress, loss of privacy, loss of peace of mind, the increased exposure to identity theft, and other economic and non-economic harm.

THIRD CAUSE OF ACTION
BREACH OF CONTRACTS TO WHICH PLAINTIFF' AND CLASS MEMBERS WERE THIRD PARTY BENEFICIARIES
Asserted on Behalf of the Nationwide Class Against Heartland

68. Plaintiff incorporates the allegations in the preceding paragraphs. This Count is brought on behalf of the **Nationwide Class.**

69. Upon information and belief, Plaintiff and Class members are intended third party beneficiaries of contracts entered into between Defendant and third parties, such as its customer merchants.

70. Upon information and belief, these contracts between Heartland and third parties require, *inter alia*, that Heartland takes appropriate steps to safeguard the Sensitive Financial Information of Plaintiff and the Class, and to promptly (and accurately) notify them when there is a breach.

71. Defendant breached these agreements, causing injury to Plaintiffs and the Class.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
Asserted on Behalf of the Nationwide Class Against Heartland

72. Plaintiff incorporates the allegations in the preceding paragraphs. This Count is brought on behalf of the **Nationwide Class.**

73. Plaintiff and Class members were required to provide Heartland with their Sensitive Financial Information in order for Heartland to provide its services on their behalf. Implicit in this transaction was a covenant for Heartland to*, inter alia*, take reasonable efforts to safeguard this information, and to take appropriate measures to promptly notify consumers in the event that this information was compromised. Indeed, Heartland recognizes these obligations, as it states on its website that the company is "deeply committed to maintaining the security of cardholder data, and we will continue doing everything reasonably possible to achieve this objective."

74. This implied contract required Defendants to not disclose the Class' private, nonpublic Sensitive Financial Information and to safeguard and protect the information from being compromised and/or stolen.

75. Defendant did not safeguard and protect Plaintiff and the Class' private, nonpublic, and financial information from being compromised and/or stolen. To the contrary, Heartland allowed this information to be disclosed to an unauthorized third party or parties.

76. Because Heartland disclosed Plaintiff and Class Members' private, non-public Sensitive Financial Information, did not inform Plaintiff and Class

members of the breach in a timely manner, and failed to safeguard and protect Plaintiff and the Class' private, nonpublic, and financial information from being compromised and/or stolen (as it implied it would through its representations about the level of security it would provide), Heartland breached its implied contract with Plaintiff and the Class.

77. Plaintiff and the Class have and/or can be expected to incur actual damages, including, but not limited to: anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

FIFTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
Asserted on Behalf of the Nationwide Class Against Heartland

78. Plaintiff incorporates the allegations in the preceding paragraphs. This Count is brought on behalf of the **Nationwide Class**.

79. Heartland owed a fiduciary duty to Plaintiff and Class members because they reposed trust and confidence in Heartland, and because Heartland possesses superior knowledge and expertise in, *inter alia*, processing and administering credit card transactions.

80. Plaintiff and Class members were required to provide Heartland (directly or indirectly) with their Sensitive Financial Information.

81. Heartland expressly or impliedly represented that it would safeguard that information.

82. Heartland failed to do so, causing damages to Plaintiff and Class members.

SIXTH CAUSE OF ACTION
NEGLIGENCE *PER SE*
Asserted on Behalf of the Nationwide Class Against Heartland

83. Plaintiff incorporates the allegations in the preceding paragraphs. This Count is brought on behalf of the **Nationwide Class**.

84. Many states have statutes and regulations that require a corporation like Heartland that has experienced a data breach to promptly notify affected consumers. For example, pursuant to New York State General Business Law § 899-aa "any person which conducts business in N.Y. state . . . must following a security breach that compromises "private information" (defined as, *inter alia*, an account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account) to disclose the breach to the affected person "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement." § 899-aa.2.

85. Heartland also failed to satisfy the minimal duty set forth in the Pennsylvania Breach of Financial Information Notification Act ("BPINA"). The BPINA requires entities that maintain or store computerized data that includes financial information to provide notice "without unreasonable delay" of any breach of the security of the system following discovery of the breach of the security of the system to any resident of Pennsylvania whose unencrypted and unredacted financial information was or is reasonably believed to have been accessed and

acquired by an unauthorized person. 73 P.S. § 2303(a). Heartland failed to notify Pennsylvania consumers without unreasonable delay.

86. Similarly, Heartland is been required to comply with the PCI standards, which required it to have, *inter alia*, adequate controls in place for preventing, detecting and responding to system intrusions.

87. These statutes, regulations, and industry security standards establish the minimal duty of care owed by the Defendant to the named Plaintiff and Plaintiff Class.

88. Defendant failed to meet that minimum duty.

89. Heartland's violations of these statutes, regulations, and industry security standards caused injury to Plaintiff and Class members.

90. The injuries suffered by Plaintiff and Class members were of the type intended to be prevented by these statutes, regulations, and industry security standards.

91. Plaintiff and Class members were members of the class of persons intended to be protected by these statutes, regulations, and industry security standards.

92. Defendant's negligence *per se* is a proximate cause of the injuries inuring to Plaintiff and the Class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of herself and all others similarly situated, respectfully request that this Court enter an Order:

(a) certifying this matter as a class action, appointing Plaintiff as Class representatives and designating Plaintiff's counsel as class counsel;

(b) granting an award against Defendant for actual, statutory, punitive, and/or compensatory damages, as provided by the New Jersey Consumer Fraud Act, and the common law and contractual claims asserted herein;

(c) granting an award against Defendant for actual, punitive and/or compensatory damages, as provided by the New Jersey Consumer Fraud Act, and enjoining Defendant from continuing their unfair and/or deceptive conduct;

(d) finding that Defendant was negligent in protecting Plaintiff's and the Class' Sensitive Financial Information, and that this conduct caused foreseeable injuries to Plaintiff and Class members;

(e) finding the Defendant was negligent *per se* by violating various statutes, regulations and industry standards, and finding that this conduct was the proximate cause of foreseeable injury to Plaintiff and Class members;

(f) finding that Defendant breached its duty to safeguard and protect Plaintiff's and the Class' Sensitive Financial Information, breached implied contracts with Plaintiff and class members, and breached contracts to which Plaintiff and class members were intended third party beneficiaries, and awarding appropriate damages;

(g) awarding damages (including punitive damages) to Plaintiff and the Class, as well as reasonable attorneys' fees and costs of litigation; and

(h) providing for such other legal and/or equitable relief as justice

requires, including an injunction or other equitable relief that requires Heartland to comply with applicable security standards.

JURY DEMAND

Plaintiffs on behalf of herself and the putative class, demand a trial by jury on all issues so triable.

Dated: January 27, 2009

Respectfully submitted,

By: CHIMICLES & TIKELLIS LLP

//s// Joseph G. Sauder

Joseph G. Sauder
Matthew D. Schelkopf
Benjamin F. Johns
One Haverford Centre
361 West Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500
Facsimile: (610) 649-3633
E-mail: JosephSauder@chimicles.com
matthewschelkopf@chimicles.com
BFJ@chimicles.com

Christopher G. Hayes
LAW OFFICE OF
CHRISTOPHER G. HAYES
225 South Church Street
West Chester, PA 19382
Telephone: (610)-431-9505
Facsimile: (610)-431-1269
E-mail: chris@chayeslaw.com

Attorneys for Plaintiffs and the Proposed Class